Remarks

Claims 1-3, 12-15, 17-19, and 26 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 5,944,794 (Okamoto et al.) "Okamoto". It is the Examiner's position as set forth in the paragraph bridging pages 3-4 of the Office Action dated March 15, 2006 that Okamoto at column 28, lines 5-65, describes "limiting the user interface of the second computer system to operate responsive to the user of the second computer system to prevent copying of the content information when such received content information is being displayed". Okamoto at column 28, lines 5-65, is copied below:

> Processing e-2: The remote file transfer program then sets up a communication path with the target computer system (home system 2) via the external access detection unit 101, the connection management unit 102, the network unit 103, and the LAN 111 of the remote system 4 to make the IP datagram communication possible, and makes the connection set up request of the TCP. In this fourth embodiment, the external access detection unit 101 on the client side is simply passed through and not operated.
>
> Processing e-3: The request is sent to the connection management unit 102 via the network unit 103 at the target computer system (home system 2) side.
>
> Processing e-4: The connection management unit 102 of the target computer system (home system 2) sets up the connection of the TCP to the transmission source computer system (remote system 4), and tries to activate the remote file transfer 206 of the home system 2 (server side).
>
> Processing e-5: The external access detection unit 101 of the home system 2 detects the above connection request, and requests the external access permission judgement unit 106B to judge whether it is possible to set up the connection. In response, the external access permission judgement unit 106B requests the network address and the user ID of the transmission source computer system (remote system 4) to the connection management unit 102.
>
> Processing e-6: The connection management unit 102 of the home system 2 has obtained the network address and the connection identifier (port number) of the transmission source computer system (remote system 4) at the step of setting up the transport layer connection, according to the protocol specification of the TCP.
>
> Processing e-7: In addition, by inquiring to the user-connection correspondence management unit 211 of the transmission source computer system (remote system 4), the external access permission judgement unit 106B of the home system 2 obtains the information such as the user ID of the transmission source computer system (remote system 4) which set up this connection. Here the processing at the user-connection correspondence management unit 211 is carried out according to the identification protocol defined by the RFC1413.
>
> Processing e-8: Also, at a time of responding from the user-connection correspondence management unit 211 of the remote system 4, the response data is encrypted by the secret key of this system itself (remote system 4) and a signature of the remote system 4 is attached at the digital signature/authentication unit 108 before it is returned. This response data contains the transmission source network address of the remote system 4 in plain text and the user ID encrypted by a secret key of the remote system 4.
>
> Processing e-9: The external access detection unit 101 of the receiving side computer system (home system 2) authenticates the data with signature from the user-connection correspondence management unit 211 of the transmission source computer system (remote system 4) at the digital signature/authentication unit 108, and then obtains two data of the transmission source network address and user ID.

It is respectfully submitted that the above citation deals with authentication for remote user access, it does not relate to any limiting of a user interface when content information is

displayed at a computer, as described in Claim 1. Nowhere in Okamoto is such feature described, or even suggested. Thus, Okamoto cannot anticipate Claim 1 since it fails to describe each and every element of Claim 1.

The Examiner contends on page 4, lines 12-14, of the Office Action of March 15, 2006 that column 25, line 62, to column 26, line 23, describes "the second computer system when displaying the decrypted content information ignores signals from the user interface capable of enabling access to the decrypted content information". Applicants copy below Okamoto at column 25, line 62, to column 26, line 23:

> From the signature for the authentication of the computer system among the received data, the authentication is carried out at the digital signature/authentication unit 108 by using the secret key of the home system 2 and the public key of the remote system 4. The secret key of the home system 2 is obtained from the secret key storage unit 109 which stores the secret key acquired from the computer system secret key storage unit 212 of the home system 2. The public key of the remote system 4 is obtained from the public key acquisition unit 110, or if it is not stored there, from the external public server (now shows) via the network unit 103. Using these two keys, the signature for the authentication of the computer system is decrypted to obtain a plain text. When the obtained plain text actually coincides with the network address of the home system 2 and the network address of the remote system 4, the authentication is successful.
>
> On the other hand, in the above operation, the authentication processing of the processing d-2 can be carried out in further detail as follows.
>
> Similarly as in a case of the processing d-1 described above, the signature for the authentication of the user ID among the received data is decrypted by using the public key of that user to obtain a plain text. When the obtained plain text actually coincides with the user ID at the transmission source computer system and the user ID at the destination computer system which are also received at the same time, the authentication is successful. Here, the public key of the user is obtained from the public key acquisition unit 110.

There is no mention at column 25, line 62, to column 26, line 23 of Okamoto of any computer system in which when displaying decrypted content information ignores signals from its user interface capable of enabling access to the decrypted content information, as described in Claim 2. In fact, nowhere in Okamoto is such feature described, or even suggested. Thus, Okamoto cannot anticipate the Claim 2, and for similar reasons Okamoto cannot anticipate Claim 18.

On page 5, lines 8-9, of the Office Action of March 15, 2006, the Examiner states that the same above citation of column 25, line 62, to column 26, line 23, Okamoto describes information that is part of a survey. However, a plain reading of this citation shows that it does not mention a survey, and is unrelated to a survey. Thus, Claim 15 also must not be anticipated by Okamoto.

Also, the Examiner contends at page 6, lines 5-9, of the Office Action of March 15, 2006 that Okamoto describes "limiting the user interface of the second computer system to operate responsive to the user of the second computer system to prevent copying of the content

information when the received content information is being displayed [column 25, lines 29-61]". The text of Okamoto at column 25, lines 29-61, is copied below:

> Processing d-1: Using the received data, the ID of the transmission source computer system (remote system 4) is authenticated.
>
> Processing d-2: Using the received data, the user ID at the transmission source computer system (remote system 4) is authenticated.
>
> Processing d-3: When the authentications by the processings d-1 and d-2 are successful, it is judged that the access is permitted as there is no access permission condition list in this third embodiment, and the access permission data as shown in FIG. 19 described above is registered into the user ID correspondence management table 105A, and the access permission is notified to the transmission source computer system (remote system 4).
>
> Here, the concrete examples of access permission data registered in the user ID correspondence management table 105A are as follows:
>
> (1) A user ID at this computer system (home system 2);
>
> (2) A network address of a corresponding external computer system (remote system 4);
>
> (3) A user ID at a corresponding external computer system (remote system 4); and
>
> (4) A valid period.
>
> Processing d-4: When the authentications by the processings d-1 and d-2 are unsuccessful, data for notifying this fact is returned to the computer system (remote system 4) which is the transmission source of the user ID correspondence establishing request.
>
> In the above operation, the authentication processing of the processing d-1 can be carried out in further detail as follows.

The above citation clearly has nothing to do with limiting the user interface of any computer to prevent copying when received content information is displayed, as described in Claim 17. Nowhere in Okamoto is this feature described, or suggested.

In regards to Claim 26, the Examiner on page 7, lines 5-9, of the Office Action of March 15, 2006, states that Okamoto at this same above citation of column 25, lines 29-61, shows that "each of the computer systems having a display and a user interface in which, when the file is played, signals from the user interface at the second computer system are ignored which enable access to the decrypted file, and when another window is selected than the window displaying the decrypted file, disables the playing of the decrypted file." However, a plain reading of Okamoto at column 25, lines 29-61, shows that this is not the case, and there is no discussion anywhere in Okamoto of a user interface such that when a file is played, signals for the user interface are ignored which enable access to such file, or that when another window is selected than the window playing a file, the playing of the file is disabled. Thus, each and every element of Claim 26 is not described by Okamoto, and Okamoto cannot anticipate Claim 26.

For the above reasons, withdrawal of the rejection of Claims 1, 2, 15, 17, 18 and 26, and their respective rejected dependent Claims 3, 12-14, and 19, is requested.

Claims 4, 5, 6-8, 9-11, and 16 were rejected as being unpatentable in view of Okamoto in combination with either U.S. Patent Nos. 6,584,199 (Kim et al.), 5,734,380 (Adams et al.), or U.S. Patent No. 6,477,504 (Hamlin et al.). Kim et al., Adams et al., and Hamlin et. al. fail to provide that absent in Claim 1 of Okamoto. Accordingly, withdrawal of the rejection of these claims is requested.

Applicants require clarification of the patent number of the secondary reference "Okamoto et al." at lines 2-3 on page 14 of the Office Action dated March 15, 2006, since it is incorrectly identified as 6,584,199.

Claims 27 and 29-41 were rejected under 35 U.S.C. §102(e) as being anticipated by U.S. Patent No. 6,102,287 (Matyas, Jr.) "Matyas". Claim 27 describes sending an encrypted information file to client computer systems for carrying out a survey received by such client computer systems. Matyas does not describe sending any encrypted file to a buyer's computer for carrying out a survey, as clear from the absence of encryption at column 19, lines 40, describing that "[a]t step 67, buyer's browser receives HTML page(s) containing survey questionnaire from the evaluator 50, and the signed certificate containing the evaluator's public key PUB_E". Applicants incorporate herein arguments over Matyas made in the Amendment filed December 23, 2005.

It is the Examiner's position at page 2, item 6, of the Office Action dated March 15, 2006, that since survey blocks are encrypted in Matyas then all surveys contained therein are encrypted. It is respectfully submitted that the Examiner in incorrect as to the use of the term "survey blocks" in Matyas. Applicants believe the Examiner is referring to "survey key blocks" of completed survey questionnaire sent from a buyer's computer to Matyas's evaluator 50 (see column 15, lines 53-63). Such "survey key blocks" are described in connection with Matyas's step 68 (FIG. 3) as explained at column 15, lines 53-63 of Matyas, which is copied below.

> FIG. 5 is a block diagram illustration of the survey protocol, which permits a buyer 10 to send a completed survey questionnaire to the evaluator 50. At step 68, the buyer 10 sends the evaluator 50 the following four data elements:
>
> 1. An encrypted key block PUB._ E(Survey1, K1, K2, Rcode_ B) 78 consisting of data elements encrypted with the public key of the evaluator 50 (PUB_ E). The data elements in the encrypted key block 78 are as follows:
>
> a. Survey1: A header indicating that the key block is a survey key block. (underline added)

See later at column 16, lines 38-44, the reason why the survey key block is encrypted is to prevent "bogus survey questionnaire responses from being accepted by the evaluator 50".

Nowhere in Matyas is there an information file encrypted which is sent for carrying out a survey of questions answerable by a user, as described in Claims 27 and 30. For similar reasons, Claim 39 also is not described by Matyas. Thus, Matyas cannot anticipate Claims 27, 30, or 39 as it fails to describe each any every element of such Claims. In view of the above, withdrawal of the rejection of Claims 27, 30, or 39, and of their respective dependent Claims 29, 31-32, and 40-41 is requested.

Matyas also does not anticipate Claim 33-38 as it fails to describe each any every element of such Claims. It is the Examiner's position that column 19, lines 24-60, of Matyas describe each and every element of Claims 33-38. Column 19, lines 24-60, of Matyas is copied below:

> At step 210, buyer's browser views purchased HTML page(s) received from seller 20. Once the buyer 10 receives a first HTML page, that page may contain `free` hyper-links to other HTML pages. The buyer 10 can continue to view the purchased HTML pages for as long as he wants, or until some prescribed time limit has been reached, according to the terms and conditions of the purchase agreement. The purchased HTML page(s) also contain a survey link that permits the buyer 10 to fill in a survey questionnaire for the purchased product. Submission of a survey questionnaire is optional, although for the purpose of describing the present invention we shall assume that the buyer 10 decides to submit a survey questionnaire.
>
> At step 212, buyer 10 points and clicks on the survey link in the purchased HTML page(s). At step 66, buyer's browser requests HTML page(s) containing survey questionnaire from the evaluator 50. At step 67, buyer's browser receives HTML page(s) containing survey questionnaire from the evaluator 50, and the signed certificate containing the evaluator's public key PUB_ E.
>
> At step 213, buyer's system validates the certificate containing the evaluator's public key PUB_ E. We assume that the certificate is signed with the public key of a certification center, and that the public key of the certification center has been previously stored in the buyer's wallet. The process of validating the signature depends on the particular signature algorithm, and is, unimportant with respect to the operation and functioning of the protocol that uses the public key PUB_ E. The received and validated public key PUB_ E is then stored in the buyer's wallet.
>
> At step 214, buyer's browser views HTML page(s) received from evaluator 50. The buyer 10 answers the questions in the survey questionnaire, and indicates that he is finished taking the survey. At step 216, buyer's system prepares a survey response, see FIG. 14. At step 68, buyers' browser sends the survey response to the evaluator 50 containing the answers to the survey questionnaire.

Clearly, the above citation does not describe each any every element of the Claim 33 system for conducting a survey. For example, it fails to describe any computer system that requests a key to decrypt an encrypted file from a network address where such key is available, receives a key when that computer system is associated with a participant selected to take a survey, and decrypts the file in accordance with such key and plays the decrypted file as part of the survey. As cited in MPEP 2131, the Federal Circuit in Verdegaal Bros. stated that "[a] claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described, in a single prior art reference" Verdegaal Bros. v. Union Oil Co. of California, 814 F2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). It is respectfully

submitted that Matyas fails to meet this standard. Withdrawal of the anticipated rejection of Claim 33 and of its dependent Claims 34-38 is thus requested.

It is believed the Application is in condition for allowance, and a notice of allowance is respectfully respected.

Respectfully submitted,

Dated: April 12, 2006

Kenneth J. LuKacher
Attorney for Applicant(s)
Registration No. 38,539

South Winton Court
3136 Winton Road South, Suite 301
Rochester, New York 14623
Telephone: (585) 424-2670
Facsimile: (585) 424-6196